Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP04/014099

International filing date: 10 December 2004 (10.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: IB
Number: PCT/IB03/06186
Filing date: 24 December 2003 (24.12.2003)

Date of receipt at the International Bureau: 25 January 2005 (25.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

WIPO OMPI

WORLD INTELLECTUAL PROPERTY ORGANIZATION
ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE

34, chemin des Colombettes, Case postale 18, CH-1211 Genève 20 (Suisse)
Téléphone: (41 22) 338 91 11 - e-mail: wipo.mail @ wipo.int. - Fac-similé: (41 22) 733 54 28

PATENT COOPERATION TREATY (PCT)
TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

CERTIFIED COPY OF THE INTERNATIONAL APPLICATION AS FILED AND OF ANY CORRECTIONS THERETO

COPIE CERTIFIÉE CONFORME DE LA DEMANDE INTERNATIONALE, TELLE QU'ELLE A ÉTÉ DÉPOSÉE, AINSI QUE DE TOUTES CORRECTIONS Y RELATIVES

International Application No. Demande internationale n°	PCT/IB 03 / 06186	International Filing Date Date du dépôt international	24 DECEMBER 2003 (24.12.03)

Geneva/Genève, 05 JANUARY 2005
(05.01.05)

**International Bureau of the
World Intellectual Property Organization (WIPO)**

**Bureau International de l'Organisation Mondiale
de la Propriété Intellectuelle (OMPI)**

BUREAU INTERNATIONAL DE L'ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
INTERNATIONAL BUREAU OF THE WORLD INTELLECTUAL PROPERTY ORGANIZATION
WIPO OMPI

J.-L. Baron
Head, PCT Receiving Office Section
Chef de la section "office récepteur du PCT"

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/IB03/06186
International Application No.

24 DECEMBER 2003 (24.12.03)
International Filing Date

INTERNATIONAL BUREAU OF WIPO
PCT International Application
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* TEL0903.WO.P0

Box No. I TITLE OF INVENTION
"USER AUTHENTICATION METHOD BASED ON THE UTILIZATION OF BIOMETRIC IDENTIFICATION TECHNICS AND RELATED ARCHITECTURE"

Box No. II APPLICANT □ This person is also inventor

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

TELECOM ITALIA S.p.A.
Piazza degli Affari, 2
I-20123 MILANO
Italy

Telephone No.
+ 39 02 85951

Facsimile No.

Teleprinter No.

Applicant's registration No. with the Office

State *(that is, country)* of nationality: IT

State *(that is, country)* of residence: IT

This person is applicant for the purposes of: □ all designated States ☒ all designated States except the United States of America □ the United States of America only □ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

BALTATU, Madalina
TELECOM ITALIA S.p.A.
Via G. Reiss Romoli, 274
I-10148 TORINO
Italy

This person is:
□ applicant only
☒ applicant and inventor
□ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: IT

State *(that is, country)* of residence: IT

This person is applicant for the purposes of: □ all designated States □ all designated States except the United States of America ☒ the United States of America only □ the States indicated in the Supplemental Box

□ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent □ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

BATTIPEDE, Francesco
PIRELLI & C. S.p.A.
Viale Sarca, 222
I-20126 MILANO
Italy

Telephone No.
+39 02 6442 3129

Facsimile No.
+39 02 6442 3190

Teleprinter No.

Agent's registration No. with the Office

□ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

See Notes to the request form

PCT/IB03/06186

Sheet No. ...2...

Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

D'ALESSANDRO, Rosalia
TELECOM ITALIA S.p.A.
Via G. Reiss Romoli, 274
I-10148 TORINO
Italy

This person is:
□ applicant only
☒ applicant and inventor
□ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:
IT

State *(that is, country)* of residence:
IT

This person is applicant for the purposes of: □ all designated States □ all designated States except the United States of America ☒ the United States of America only □ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

D'AMICO, Roberta
TELECOM ITALIA S.p.A.
Via G. Reiss Romoli, 274
I-10148 TORINO
Italy

This person is:
□ applicant only
☒ applicant and inventor
□ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:
IT

State *(that is, country)* of residence:
IT

This person is applicant for the purposes of: □ all designated States □ all designated States except the United States of America ☒ the United States of America only □ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
□ applicant only
□ applicant and inventor
□ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: □ all designated States □ all designated States except the United States of America □ the United States of America only □ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
□ applicant only
□ applicant and inventor
□ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: □ all designated States □ all designated States except the United States of America □ the United States of America only □ the States indicated in the Supplemental Box

□ Further applicants and/or (further) inventors are indicated on another continuation sheet.

See Notes to the request form

Sheet No. ...3...

Box No. V DESIGNATION OF STATES *Mark the applicable check-boxes below; at least one must be marked.*

The following designations are hereby made under Rule 4.9(a):

Regional Patent

☒ AP **ARIPO Patent: GH** Ghana, **GM** Gambia, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **MZ** Mozambique, **SD** Sudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** United Republic of Tanzania, **UG** Uganda, **ZM** Zambia, **ZW** Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* ....

☒ EA **Eurasian Patent: AM** Armenia, **AZ** Azerbaijan, **BY** Belarus, **KG** Kyrgyzstan, **KZ** Kazakhstan, **MD** Republic of Moldova, **RU** Russian Federation, **TJ** Tajikistan, **TM** Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ EP **European Patent: AT** Austria, **BE** Belgium, **BG** Bulgaria, **CH & LI** Switzerland and Liechtenstein, **CY** Cyprus, **CZ** Czech Republic, **DE** Germany, **DK** Denmark, **EE** Estonia, **ES** Spain, **FI** Finland, **FR** France, **GB** United Kingdom, **GR** Greece, **IE** Ireland, **IT** Italy, **LU** Luxembourg, **MC** Monaco, **NL** Netherlands, **PT** Portugal, **SE** Sweden, **SI** Slovenia, **SK** Slovakia, **TR** Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☒ OA **OAPI Patent: BF** Burkina Faso, **BJ** Benin, **CF** Central African Republic, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroon, **GA** Gabon, **GN** Guinea, **GQ** Equatorial Guinea, **GW** Guinea-Bissau, **ML** Mali, **MR** Mauritania, **NE** Niger, **SN** Senegal, **TD** Chad, **TG** Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* ....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☒ **AE** United Arab Emirates ....
☒ **AG** Antigua and Barbuda
☒ **AL** Albania ....
☒ **AM** Armenia ....
☒ **AT** Austria ....
☒ **AU** Australia ....
☒ **AZ** Azerbaijan ....
☒ **BA** Bosnia and Herzegovina ....
☒ **BB** Barbados
☒ **BG** Bulgaria ....
☒ **BR** Brazil ....
☒ **BY** Belarus ....
☒ **BZ** Belize ....
☒ **CA** Canada
☒ **CH & LI** Switzerland and Liechtenstein
☒ **CN** China ....
☒ **CO** Colombia
☒ **CR** Costa Rica ....
☒ **CU** Cuba ....
☒ **CZ** Czech Republic ....
☒ **DE** Germany ....
☒ **DK** Denmark ....
☒ **DM** Dominica
☒ **DZ** Algeria ....
☒ **EC** Ecuador ....
☒ **EE** Estonia ....
☒ **ES** Spain ....
☒ **FI** Finland ....
☒ **GB** United Kingdom
☒ **GD** Grenada
☒ **GE** Georgia ....
☒ **GH** Ghana ....

☒ **GM** Gambia
☒ **HR** Croatia ....
☒ **HU** Hungary ....
☒ **ID** Indonesia
☒ **IL** Israel ....
☒ **IN** India ....
☒ **IS** Iceland
☒ **JP** Japan ....
☒ **KE** Kenya ....
☒ **KG** Kyrgyzstan ....
☒ **KP** Democratic People's Republic of Korea ....
☒ **KR** Republic of Korea ....
☒ **KZ** Kazakhstan ....
☒ **LC** Saint Lucia
☒ **LK** Sri Lanka
☒ **LR** Liberia
☒ **LS** Lesotho ....
☒ **LT** Lithuania
☒ **LU** Luxembourg
☒ **LV** Latvia
☒ **MA** Morocco ....
☒ **MD** Republic of Moldova ....
....
☒ **MG** Madagascar ....
☒ **MK** The former Yugoslav Republic of Macedonia ....
☒ **MN** Mongolia
☒ **MW** Malawi ....
☒ **MX** Mexico ....
☒ **MZ** Mozambique ....
☒ **NO** Norway

☒ **NZ** New Zealand ....
☒ **OM** Oman
☒ **PH** Philippines ....
☒ **PL** Poland ....
☒ **PT** Portugal ....
☒ **RO** Romania
☒ **RU** Russian Federation ....
....
☒ **SC** Seychelles
☒ **SD** Sudan
☒ **SE** Sweden
☒ **SG** Singapore
☒ **SK** Slovakia ....
☒ **SL** Sierra Leone ....
☒ **TJ** Tajikistan ....
☒ **TM** Turkmenistan ....
☒ **TN** Tunisia
☒ **TR** Turkey ....
☒ **TT** Trinidad and Tobago ....
....
☒ **TZ** United Republic of Tanzania
☒ **UA** Ukraine ....
☒ **UG** Uganda ....
☒ **US** United States of America ....
....
☒ **UZ** Uzbekistan ....
☒ **VC** Saint Vincent and the Grenadines
☒ **VN** Viet Nam ....
☒ **YU** Yugoslavia ....
☒ **ZA** South Africa ....
☒ **ZM** Zambia
☒ **ZW** Zimbabwe ....

Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:

☐ .... ☐ .... ☐ ....
☐ .... ☐ .... ☐ ....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Sheet No. ...4...

Supplemental Box *If the Supplemental Box is not used, this sheet should not be included in the request.*

1. *If, in any of the Boxes, except Boxes Nos. VIII(i) to (v) for which a special continuation box is provided,* ***the space is insufficient*** *to furnish all the information: in such case, write "Continuation of Box No...." (indicate the number of the Box) and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:*

(i) ***if more than two persons are to be indicated as applicants and/or inventors*** *and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;*

(ii) *if, in Box No. II or in any of the sub-boxes of Box No. III, the indication* ***"the States indicated in the Supplemental Box"*** *is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;*

(iii) *if, in Box No. II or in any of the sub-boxes of Box No. III,* ***the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America:*** *in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;*

(iv) *if, in addition to the agent(s) indicated in Box No. IV, there are* ***further agents:*** *in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;*

(v) *if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication* ***"patent of addition,"*** *or* ***"certificate of addition,"*** *or if, in Box No. V, the name of the United States of America is accompanied by an indication* ***"continuation"*** *or* ***"continuation-in-part":*** *in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;*

(vi) *if, in Box No. VI, there are* ***more than five earlier applications whose priority is claimed:*** *in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI.*

2. *If, with regard to the* ***precautionary designation statement*** *contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.*

Continuation of BOX No. IV

ADDITIONAL AGENTS:

Carlo BOTTERO, Pier Giovanni GIANNESI, Paolo MARKOVINA

PIRELLI & C. S.p.A.
Viale Sarca, 222
I-20126 MILANO
Italy

All enrolled at the Register of Italian Patent Attorneys

Sheet No. . . .5. . .

Box No. VI PRIORITY CLAIM

The priority of the following earlier application(s) is hereby claimed:

Filing date of earlier application *(day/month/year)*	Number of earlier application	Where earlier application is:		
		national application: country or Member of WTO	regional application:* regional Office	international application: receiving Office
item (1)				
item (2)				
item (3)				
item (4)				
item (5)				

□ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as:

□ all items □ item (1) □ item (2) □ item (3) □ item (4) □ item (5) □ other, see Supplemental Box

* *Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):* . . . .

. . . .

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)*:

ISA / EP . . . .

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date *(day/month/year)* Number Country *(or regional Office)*

Box No. VIII DECLARATIONS

The following **declarations** are contained in Boxes Nos. VIII (i) to (v) *(mark the applicable check-boxes below and indicate in the right column the number of each type of declaration)*:

			Number of declarations
□	Box No. VIII (i)	Declaration as to the identity of the inventor	:
□	Box No. VIII (ii)	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	:
□	Box No. VIII (iii)	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	:
□	Box No. VIII (iv)	Declaration of inventorship (only for the purposes of the designation of the United States of America)	:
□	Box No. VIII (v)	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	:

See Notes to the request form

PCT/IB03/06186

Sheet No. ...6...

Box No. IX CHECK LIST; LANGUAGE OF FILING

This international application **contains**:

(a) **in paper form,** the following number of sheets :

request (including declaration sheets)	:	6
description (excluding sequence listings and/or tables related thereto)	:	23
claims	:	9
abstract	:	1
drawings	:	3
Sub-total number of sheets	:	42
sequence listings	:	
tables related thereto	:	
(for both, actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (c) below)		
Total number of sheets	:	42

(b) □ **only in computer readable form** (Section 801(a)(i))

(i) □ sequence listings

(ii) □ tables related thereto

(c) □ **also in computer readable form** (Section 801(a)(ii))

(i) □ sequence listings

(ii) □ tables related thereto

Type and number of carriers (diskette, CD-ROM, CD-R or other) on which are contained the

□ sequence listings: ....

□ tables related thereto: ....

(additional copies to be indicated under items 9(ii) and/or 10(ii), in right column)

This international application is **accompanied by** the following item(s) *(mark the applicable check-boxes below and indicate in right column the number of each item):* Number of items

1. □ fee calculation sheet :
2. □ original separate power of attorney :
3. □ original general power of attorney :
4. □ copy of general power of attorney; reference number, if any: .... :
5. □ statement explaining lack of signature :
6. □ priority document(s) identified in Box No. VI as item(s): .... :
7. □ translation of international application into *(language)*: .... :
8. □ separate indications concerning deposited microorganism or other biological material :
9. □ sequence listings in computer readable form *(indicate type and number of carriers)*
   (i) □ copy submitted for the purposes of international search under Rule 13*ter* only (and not as part of the international application) :
   (ii) □ *(only where check-box (b)(i) or (c)(i) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Rule 13*ter* :
   (iii) □ together with relevant statement as to the identity of the copy or copies with the sequence listings mentioned in left column :
10. □ tables in computer readable form related to sequence listings *(indicate type and number of carriers)*
    (i) □ copy submitted for the purposes of international search under Section 802(b-*quater*) only (and not as part of the international application) :
    (ii) □ *(only where check-box (b)(ii) or (c)(ii) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Section 802(b-*quater*) :
    (iii) □ together with relevant statement as to the identity of the copy or copies with the tables mentioned in left column :
11. □ other *(specify)*: .... :

Figure of the drawings which should accompany the abstract: Fig. 1

Language of filing of the international application: Italian

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Francesco Battipede

BATTIPEDE, Francesco

December 24, 2003

For receiving Office use only

1. Date of actual receipt of the purported international application: 24 DECEMBER 2003 24. 12. 03

2. Drawings:

□ received:

□ not received:

3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:

4. Date of timely receipt of the required corrections under PCT Article 11(2):

5. International Searching Authority (if two or more are competent): ISA /

6. □ Transmittal of search copy delayed until search fee is paid

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

TRANSLATION (RULE 12.3)

USER AUTHENTICATION METHOD BASED ON THE UTILIZATION OF BIOMETRIC IDENTIFICATION TECHNICS AND RELATED ARCHITECTURE

* * * * *

The present invention refers in general to the field of secure authentication system. More particularly, the present invention refers to a user authentication method based on the utilization of biometric identification technics and related architecture.

Authentication is the process by which an entity, such as a financial institution, a bank, etc., identifies and verifies its customers or users to itself and identifies and verifies itself to its customers or users.

Authentication includes the use of physical objects, such as cards and/or keys, shared secrets, such as Personal Identification Numbers (PIN's) and/or passwords, and biometric technologies such as voice prints, photos, signatures and/or fingerprints. Biometric tasks include, for example, an identification task and a verification task. The verification task determines whether or not the person claiming an identity is really the person whose identity has been claimed.

The identification task determines whether the biometric signal, such as a fingerprint, matches that of someone already enrolled in the system.

Various biometrics have been considered for use with smartcards, such as fingerprints, hand prints, voice prints, retinal images, handwriting samples and the like.

An example of a biometric-based smartcard is shown in US-A-5,280,527 describing a credit card sized token (referred to as biometric security apparatus) containing a microchip, in which a sample of the authorised user's voice is stored. In order to gain access to an account, the user must insert the token into a designated slot of an ATM, and then speak with the ATM. If a match is found between the user's voice and the sample enrolment of the voice stored into the microchip, access to the account is granted.

Although the system disclosed in US-A-5,280,527 reduces the risks of unauthorised access, if compared with conventional PIN-based systems, however, to the extent that the credit card and the microchip disposed therein can be tampered with, the system does not provide the level of reliability and security that is often required in nowadays finance transactions.

In WO-A-0139134 a security system is further disclosed, comprising: a central unit with a biometric sensor to detect biometric data representing characteristic biometric features of a person; at least one portable data carrier; a memory means for storing biometric reference data representing the biometric reference features of the person in the system; a control system capable of generating an authorisation signal to control a functional unit depending on a comparison between the biometric data detected by the sensor and the reference data.

In the security system proposed in such document, the reference data, that are compared with the biometric data detected by the sensor to ascertain the authenticity of the user, are not wholly stored into the data carrier, in the conventional manner, but are splitted, partly in the data carrier and partly in the reading device. Only the combination of data carrier and reading device will produce the complete information needed for authentication.

The invention is particularly advantageous if the biometric sensor is a fingerprint sensor. A fingerprint sensor determines the locally resolved position of minutiae of the fingerprint. The minutiae are singular points of the papillary lines of a fingerprint. These might be end points, branches or similar points of the papillary lines of the fingerprint. The local position is determined depending on the distance from a reference point or radius to the angle related to a reference direction.

In order to personalise the data carrier, the fingerprint of the data carrier owner is reproduced and appropriate reference values are determined for radius and angle. These values are then stored into the system. For practical purpose, the radius reference data are stored only on the data carrier and the angle reference data are stored only on the reading device. Alternatively, the angle reference data are stored in the data carrier and the distance reference data are stored on the reading device.

The Applicant faced the problem of realising a method for authenticating users based on the use of biometric identification technics, that is secure, independent from the used biometric identification technics and that protects user privacy.

The Applicant has observed that the above-described problem can be solved by a user authentication method based on the use of biometric identification technics comprising the steps of: generating a reference biometric template from a first biometric image of a user to be authenticated and, afterwards, splitting the reference biometric template into a first and a second reference biometric template portion, said first and second reference biometric template portion being separable. The first and the second biometric reference template portion are then signed, ciphered and stored in different memories.

More specifically, a user authentication method based on the use of biometric identification technics comprises an enrolment step and a verification step, said enrolment step including the steps of:

- generating a reference biometric template from a first biometric image of a user to be authenticated;
- splitting said reference biometric template into a first and a second reference biometric template portion;
- ciphering said first and second reference biometric template portion; and
- storing each one of said reference biometric template portions into a different memory.

Another aspect of the present invention refers to an architecture based on the use of biometric identification technics comprising:

- at least one data enrolment system for generating a reference biometric template from a first biometric image of a user to be authenticated, said data enrolment system comprising a Host Computer for splitting said reference biometric template into a first and a second reference biometric template portion that are physically separable and for ciphering said first and second reference biometric template portion;

- at least one portable data carrier associated with said user to be authenticated, said data carrier comprising a memory for storing said first signed and ciphered reference biometric template portion; and

- at least one data verification system comprising a memory for storing said second signed and ciphered reference biometric template portion.

Another aspect of the present invention refers to a portable data carrier associated with a user that has to be authenticated through a user authentication architecture, said data carrier including a microprocessor comprising a memory for storing a first reference biometric template portion associated with said user to be authenticated, said first reference biometric template portion being signed and ciphered, said portable data carrier being adapted to received as input, from said user authentication architecture, a second reference biometric template portion and a template live associated with said user to be authenticated, said second reference biometric template portion and said template live being signed and ciphered, said microprocessor further comprising:

- a processing logic for ciphering said first and second reference biometric template portion and for recomposing therefrom said reference biometric template associated with said user to be authenticated;

- a comparing logic for comparing said reference biometric template recomposed with said template live and sending a result of said comparison to said user authentication architecture.

Another aspect of the present invention refers to a data verification system comprising an electronic device and a portable data carrier associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and ciphered;

said electronic device comprising:

- a memory adapted to store a second reference biometric template portion associated with a user to be authenticated, complementary with said first portion, said second reference biometric template portion being signed and ciphered;
- an image acquiring and processing device for generating a template live;

said electronic device being adapted to cipher and sign said template live, transmit said second reference biometric template portion and said template live to said portable data carrier and authenticate said user depending on the result of a comparison performed by said data carrier between said template live and a reference biometric template of said user to be authenticated, said reference biometric template being recomposed by using said first and second reference biometric template portion.

A further aspect of the present invention deals with a computer program product that can be loaded in the memory of at least one electronic processor and comprising portions of software code to perform the process according to the invention when the product is executed on a processor: in this context such diction must be deemed equivalent to the mention of a means readable by a computer comprising instructions to control a network of computers in order to perform a process according to the invention. The reference to "at least one electronic processor" is obviously aimed to point out the possibility of carrying out the solution according to the invention in a de-centralised context.

Further preferred aspects of the present invention are disclosed in the dependent claims and in the present description.

The features and the advantages of the present invention will result from the herein below description of an embodiment, provided as a non-limiting example, with reference to the enclosed drawings, in which:

- figure 1 is a schematic representation of a user authentication architecture according to the invention;
- figure 2 shows a flow diagram related to implementing a first step of a user authentication method according to the invention; and
- figure 3 shows a flow diagram related to implementing a second step of the user authentication method according to the invention.

With reference to figure 1, the user authentication method according to the invention is applied to a user authentication architecture 1 comprising a data enrolment system 2, a data verification system 3 and a portable data carrier 4, this latter one belonging to a user that has to be authenticated. The data carrier 4 can be a substrate whose sizes are substantially rectangular, such as for example an access card, a credit card, a debit card, an identification card, a smart card, a SIM card. The data carrier 4 is equipped with a microprocessor 5 including a processing logic 5a, a comparing logic 5b and a memory 6.

Always with reference to figure 1, in a preferred embodiment, the data enrolment system 2 comprises a Host Computer 7, for example a personal computer, a business computer, etc., having enough memory 7a to store biometric data of a user that has to be authenticated. The data enrolment system 2 can also include an image acquiring and processing device 8, connected to the Host Computer 7, and a data reading/writing device 60, also connected to the Host Computer 7 realising the interface with the data carrier 4. The data reading/writing device 60 can be, for example, a smart card reader, if the data carrier 4 is a smart card, or a cellular phone, if the data carrier 4 is a SIM card.

Specifically, the image acquiring and processing device 8 includes: a sensor 9 of the biometric type, for example a television camera, to detect a first biometric image of the user that has to be authenticated, for example a face template; an image processor 10, connected between sensor 9 and Host Computer 7, to generate a reference biometric template from the user biometric image, detected through sensor 9.

Preferably, the data enrolment system 2 is a separated system from the data verification system 3 and is placed in a secure environment.

In a preferred embodiment, the data verification system 3 comprises an electronic device 11, for example a personal computer, a palmtop computer, a cellular telephone, an hand-held PC, a smart-phone, having enough memory 11a to store biometric data of a user that has to be authenticated.

The data verification system 3 can also comprise: a data base, of a known type and therefore not shown in figure 1, managed by a remote system connected to the electronic device 11; an image acquiring and processing device 12; a data reading/writing device 61 realising the interface with the data carrier 4. The image acquiring and processing device 12 and the data reading/writing device 61 are both connected to the electronic device 11. Moreover, the data reading/writing device 61 can be, for example, a smart card reader, if the data carrier 4 is a smart card, or a cellular phone, if the data carrier 4 is a SIM card.

Specifically, the image acquiring and processing device 12 comprises: a sensor 13, of the biometric type, for example a television camera, to detect a second biometric image (the face template) of the user that has to be authenticated. The image acquiring and processing device 12 also includes an image processor 14, connected between sensor 13 and electronic device 11, to generate a template live from the user biometric image detected through the sensor 13. The electronic device 11 can also comprise a processing logic (not shown in figure 1) able to read and interpret the comparison operation result between reference biometric template and template live performed by the data carrier 4, as will be described more in detail below.

It is better to state that, in the following description, for ciphering and deciphering biometric data, cryptographic algorithms of the asymmetrical type, for example the RSA algorithm, are preferably used. In particular, these algorithms are based on the use of two different keys in the data ciphering and deciphering steps and on the existence of a PKI (Public Key Infrastructure), for example based on standard X.509 described in R. Housley, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999.

The user authentication method, according to the invention, will now be described with reference to the flow diagrams shown in figures 2-3.

In a preferred embodiment, the method according to the invention comprises an enrolment step 20, performed by the data enrolment system 2 and shown in figure 2, and a verification step 40, performed by the data verification system 3 and the data carrier 4 and shown in figure 3.

With reference to figure 2, initially the enrolment step 20 provides an initialisation step 21 of the data enrolment system 2, of the data verification system 3 and the data carrier 4.

Specifically, the initialisation step 21 provides:

- storing, in the memory 7a of Host Computer 7, a pair of public KE_{pub} and private KE_{pr} keys associated with the data enrolment system 2, the related digital certificate C_E containing the public key KE_{pub} signed with the private key issued by a secure Certification Authority and, possibly, the digital certificate C_{AC} of the same Certification Authority;

- storing, in the memory 6 of data carrier 4, a pair of public KU_{pub} and private KU_{pr} keys associated with the user to be authenticated, the related digital certificate C_U containing the public key KU_{pub} signed with the private key of the secure Certification Authority and, possibly, the digital certificate C_{AC} of the same Certification Authority. Alternatively, the data carrier 4 initialisation can provide for the generation of the pair of public and private keys KU_{pub}, KU_{pr} aboard the data carrier 4 itself (on-card) and the transmission of the certification request for the public key KU_{pub} to the secure Certification Authority. The initialisation process is then finalised by installing the user digital certificate C_U on the data carrier 4 and distributing the related certificate to the data enrolment system 2 and the data verification system 3. All these operations can be performed in the microprocessor 5; and

- storing, in the memory 11a of electronic device 11, a file containing a pair of public KV_{pub} and private KV_{pr} keys associated with the data verification system 3, the related digital certificate C_V containing the public key KV_{pub} signed with the private key issued by the secure Certification Authority and, possibly, the digital certificate C_{AC} of the same Certification Authority.

The enrolment step 20 then proceeds with detecting, through the sensor 9, a first biometric image of the user to be authenticated (block 22). Afterwards, the first biometric image is transferred to the image processor 10 that generates the reference biometric template (block 23).

The reference biometric template is then stored into the memory 7a of the Host Computer 7 (block 24).

Afterwards, the Host Computer 7 decomposes the reference biometric template into a first and a second reference biometric template portion (block 25), using a splitting algorithm that will be described more in detail herein below, and then destroys the original copy of the reference biometric template (block 26).

At this time, the Host Computer 7 signs the first and the second reference biometric template portion with the private key KE_{pr} of the data enrolment system 2 (block 27) and then ciphers the two portions with the public key KU_{pub} of the user to be authenticated (block 28).

Afterwards, the Host Computer 7 transfers the first reference biometric template portion onto the data carrier 4 (block 29). Here, the first reference biometric template portion is stored into a protected area 6a (shown in figure 1) of the memory 6 (block 30). For example, the memory 6a area can be protected through PIN.

Communication between data enrolment system 2 and data carrier 4 can occur for example though the communication protocol implemented in the reading/writing device 60. The reading/writing device 60 is also equipped with a logic (an application program) that checks the data transfer.

The second reference biometric template portion is instead transferred and stored into the memory 11a of the electronic device 11 (block 31).

Alternatively, the second reference biometric template portion can be transferred and stored into the data base.

The transfer of the second reference biometric template portion from data enrolment system 2 to electronic device 11, or to data base, can occur by using methods of the OOB ("Out Of Band") type. In particular, these methods assume that data are not transferred in a network, but are transferred using alternative communication channels, such as, for example, a telephone channel or the traditional mail.

Less preferably, the transfer of the second reference biometric template portion can occur through a modem or a communication network, for example a TCP/IP or GSM network.

With reference now to figure 3, the verification step 40 starts when a user, by entering the data carrier 4 into the data reading/writing device 61, asks the user architecture 1 to be authenticated (block 40a). Under these conditions, the data verification system 3, through the sensor 13, detects a second biometric image of the user that has to be authenticated (block 41). This second biometric image is then transferred to the image processor 14 that generates the template live (block 42). Afterwards, the template live is sent to the electronic device 11 that signs it with the private key KV_{pr} of the data verification system 3 and ciphers it with the public key of the user KU_{pub} (block 43).

At that time, the electronic device 11, through the reading/writing device 61, transmits to the data carrier 4 both the template live and the second reference biometric template portion, this latter one stored locally or recovered by the data base, enclosing a univocal Nonce (namely an aleatory value, used a single time in a cryptographic scheme) to guarantee the authenticity of the current data verification session (block 44). The univocal Nonce is also ciphered and signed. Such operation guarantees for example the protection from the so-called replay attacks (attacks where the attacking person is an authorised user that re-proposes to the system, in a following authentication session, a previously positive authentication session as regards the interested user).

Communication between data verification system 3 and data carrier 4 can occur for example through the communication protocol implemented in the reading/writing device 61. The reading/writing device 61 is also equipped with a logic (an application program) that checks the data transfer.

Afterwards, the data carrier 4, using its own private key KU_{pr}, deciphers the second reference biometric template portion and checks its signature by using the public key KE_{pub} of the data enrolment system 2 (block 45). In case of check success, the data carrier 4, through a re-composition algorithm, stored into the memory 6 and shown below, re-composes the reference biometric template (block 46) using the now deciphered second reference biometric template portion and the first reference biometric template portion, stored into the protected memory area 6a.

Afterwards, the data carrier 4, using its own private key KU_{pr}, deciphers the template live transmitted by the data verification system 3 and checks its signature by using the public key KV_{pub} of the data verification system 3 (block 47).

If all previously-described check operations realised through the processing logic 5a of the microprocessor 5, have a positive result, the data carrier 4 performs a comparison operation between the reference biometric template and the template live (block 48).

Preferably, the comparison operation is performed by the comparing logic 5b of the microprocessor 5 as an atomic operation using known comparison functions depending on the biometric identification technics used. For example, for the face template, as comparison functions, those provided in the Principal Component Analysis (Eigenfaces) or Local Features Analysis, or Neural Networks or 3D or wavelet Gabor, etc. technics can be used.

Afterwards, the data carrier 4 transfers to the data verification system 3 the comparison operation result together with the univocal Nonce previously received by the data verification system itself (block 49).

The comparison operation result and the univocal Nonce can for example be sent as a message signed with the user private key Ku_{pr} and ciphered with the public key KV_{pub} of the data verification system 3.

At this time, the electronic device 11, using the private key KV_{pr} of the data verification system 3, deciphers the message sent thereto by the data carrier 4, checks its signature, and, depending on the comparison operation result, grants or not the user access to the required service (block 50).

In case a data base is used for storing the second reference biometric template portion, it is necessary to make secure also the communication between electronic device 11 and remote data base managing system. This can be obtained by using, for example, the previously-described authentication, privacy and non-repudiation cryptographic mechanisms, in order to guarantee the authentication of affected parts, in addition to integrity and privacy of transferred data.

Moreover, the remote data base managing system can use access control methods, of the Access Control List type (with user authentication through userID and Password or through digital certificates) to guarantee a secure access to data contained in the data base.

Preferably, the splitting algorithm used by the data enrolment system 2 to split the reference biometric template into the two portions of reference biometric template, is a secret splitting algorithm, that can be used in the cryptographic techniques of the "secret sharing scheme" type. In this case a secret is divided into N parts, securely transferred to N entities with the property that, starting from a single part of the secret, the original cannot be rebuilt. An algorithm of this type is for example described in H. Feistel in "Cryptographic Coding for Data-Banking Privacy", IBM Research, New York, 1970.

More in detail, the splitting algorithm comprises an enrolment step in which the data enrolment system 2 that created the template t (the reference biometric template) generates a random number t_1 (the first reference biometric template portion) of the same size (length) of the template t. Afterwards the data enrolment system 2 applies a XOR function to t and t_1 to generate a value t_2 (the second reference biometric template portion), namely:

t XOR $t_1 = t_2$

t_1 is then stored in a protected mode (that provides for signature and ciphering) on the data carrier 4 while t_2 is stored in a protected mode (that provides for signature and ciphering) on the data verification system 3 or in the central data base.

The re-composition algorithm for the template t, used by the data carrier 4 to re-compose the template t from t_1 and t_2, is, mathematically, the reverse function of the previously-described splitting algorithm. In particular, the data carrier 4, after having obtained t_2, performs the XOR between t_1 and t_2 rebuilding the original value of the template t, namely:

t_1 XOR $t_2 = t$.

If all described operations are correctly performed, the technic is secure since by possessing a single part, t1 or t2, it is not possible to go back to the template t.

The advantages that can be obtained with the described user authentication method are as follows.

Firstly, the user authentication method is secure since an hacker that tries to violate either the data carrier 4 or the data verification system 3 does not obtain enough elements to go back to the reference biometric template, since this latter one is partly stored in the data carrier 4 and partly in the data verification system 3. In this way, both user privacy compliance, and the chance of using the same biometric technic also in case of violation/corruption of only one part of the reference biometric template, are guaranteed. In fact, the reference biometric template is a piece of information depending on the used biometric technic: by applying the same biometric technic to the image of the same person, a reference biometric template is obtained that is very similar to the original one. Therefore, if the whole reference biometric template falls in the hand of an hacker, this latter one could use it for disguising as the user enabled to the service, impairing the used biometric technic. Moreover, it is plausible that, through a reverse-engineering process, the hacker can go back to the mode used by the biometric technic to produce the reference biometric template. In this way, the relevant biometric technic is no more secure.

Moreover, the user authentication method according to the invention is also advantageous in case the authentication is mandatory for the access to an on-line service, in which the operator providing the service controls the data verification system 3. In fact, the operator offering the service can go on keeping the control over the verification of the users because, according to the invention, both data carrier 4 and data verification system 3 concur in performing the verification step in a secure way that cannot be repudiated (the non-repudiation of a session implies the impossibility for a user to negate having participated into the session itself).

Moreover, the global security provided by the user authentication method according to the invention is further increased by the fact that the creation logic of the reference biometric template 11 does not reside on the data carrier 4 but on the data enrolment system

2 that, preferably, is a separate system from the data verification system 3 and placed in a secure environment. On the data carrier 4 there are only the processing logic 5a that re-composes the reference biometric template and also performs the suitable cryptographic operations and the comparing logic 5b computing the correlation between reference biometric template and template live.

It is finally clear that to the herein described and shown user authentication method and its related architecture numerous modifications and variations can be made, all falling within the scope of the inventive concept, as defined in the enclosed claims.

For example, biometric technics can be used that are different from face recognition, such as fingerprints, hand prints, voice templates, retinal images, calligraphic samples and the like.

Moreover, the user authentication method according to the invention can be applied to different scenarios, such as for example:

- Stand Alone scenario, in which the user authentication method according to the invention is used to protect the access to the data verification system 3 (ex. login to personal computer, palmtop, cellular phone-SIM) by a user provided with the data carrier 4;
- client-server scenario, in which the client scenario comprises the data carrier 4, preferably realises as a SIM-card, and a client portion of the data verification system 3, while the server scenario comprises a server portion of the data verification system 3. In particular, the server portion of the data

verification system 3 can coincide or not with a central server (for example the server offering the required service). In this case, the client portion of the data verification system 3 can perform a more or less active role in the authentication process. For example, the client portion of the data verification system 3 can perform the function of detecting the biometric image of the user that has to be authenticated, then transferring it to the central server to which instead the template live generation is entrusted; the central server will then take care of transferring the template live to the client portion of the data verification system 3.

Alternatively, the client portion of the data verification system 3 can also generate the template live.

In both scenarios taken into account, the comparison operation between reference biometric template and template live is performed on the data carrier 4, then the recomposed reference biometric template never goes out of the data carrier 4. The result of this operation is then transferred in a secure way (for example ciphered and signed) to the central server that decides whether granting or not the authorisation.

CLAIMS

1. User authentication method based on the use of identification biometric technics comprising an enrolment step (20) and a verification step (40), said enrolment step (20) including the steps of:

- generating (22, 23) a reference biometric template from a first biometric image of a user to be authenticated;
- splitting (25) said reference biometric template into a first and a second reference biometric template portion;
- ciphering (27, 28) said first and second reference biometric template portion; and
- storing (29, 30, 31) each one of said reference biometric template portions into a different memory.

2. Method according to Claim 1, characterised in that said step of storing each one of said reference biometric template portions into a different memory comprises the step of:

- transmitting (29) said first reference biometric template portion from a first system (2) to a device (4), said first system (2) operating in said enrolment step (20);
- storing (30) said first reference biometric template portion into a memory (6) of said device (4), said device (4) operating in said verification step (40);
- transmitting (31) said second reference biometric template portion from said first system (2) to a second system (3), said second system (3) operating in said verification step (40); and

- storing (31) said second reference biometric template portion into a memory (11a) of said second system (3).

3. Method according to any one of Claims 1 or 2, characterised in that said verification step (40) comprises the steps of:

- generating (41, 42) a template live from a second biometric image of said user to be authenticated;
- ciphering (43) said template live; and
- transmitting (44) said template live and said second reference biometric template portion to said device (4).

4. Method according to Claim 3, characterised in that said verification step (40) comprises the steps of:

- deciphering (45, 47) said template live and said second reference biometric template portion;
- re-composing (46) said reference biometric template from said first and second reference biometric template portion; and
- comparing (48) said re-composed reference biometric template with said template live.

5. Method according to Claim 4, characterised in that said verification step (40) comprises the steps of:

- sending (49) a result of said comparison to said second system (3); and
- authenticating (50) or not authenticating said user depending on said result.

6. Method according to any one of Claims 2-5, characterised in that said step of splitting said

reference biometric template into a first and a second reference biometric template portion comprises the step of:

- destroying said biometric template performed by said first system (2).

7. Method according to any one of Claims 2-6, characterised in that said step of ciphering (27, 28) said first and second reference biometric template portion comprises the steps of:

- storing (21) a first and a second key (KE_{pub}, KE_{pr}) and a related digital certificate (C_E) into a memory (7a) of said first system (2), said first and second keys (KE_{pub}, KE_{pr}) being respectively a public key (KE_{pub}) and a private key (KE_{pr}) associated with said first system (2);

- storing (21) a first and a second key (KU_{pub}, KU_{pr}) and a related digital certificate (C_u) into said memory (6) of said device (4), said first and second keys (KU_{pub}, KU_{pr}) being respectively a public key (KU_{pub}) and a private key (KU_{pr}) associated with said user to be authenticated;

- signing (27) said first and second reference biometric template portion with said private key (KE_{pr}) of said first system (2); and

- ciphering (28) said first and second reference biometric template portion with said public key (KU_{pub}) of said user to be authenticated.

8. Method according to any one of Claims 3-7, characterised in that said step of transmitting said template live and said second reference biometric template portion to said device (4) comprises the steps of:

- generating an aleatory value associated with the current data verification step (40), said aleatory value guaranteeing the authenticity of said current data verification step (40);

- signing and ciphering said aleatory value; and

- transmitting said aleatory value to said device (4).

9. Method according to Claims 7 or 8, characterised in that said step of ciphering said comparison biometric template comprises the steps of:

- storing a first and a second key (KV_{pub}, KV_{pr}) and a related digital certificate (C_V) into said memory (11a) of said second system (3), said first and second keys (KV_{pub}, KV_{pr}) being respectively a public key (KV_{pub}) and a private key (KV_{pr}) associated with said second system (3);

- signing (43) said template live with said private key (KV_{pr}) of said second system (3); and

- ciphering (43) said template live with said public key (KU_{pub}) of said user to be authenticated.

10. Method according to any one of Claims 8 or 9, characterised in that said step of deciphering said template live and said second reference biometric template portion comprises the steps of:

- deciphering the signature and the validity of said aleatory value;

- deciphering (45) said second reference biometric template portion with said private key (KU_{pr}) of said user to be authenticated;

- verification its signature (45)

- deciphering (47) said template live with said private key (KU_{pr}) of said user to be authenticated; and

- verification its signature (47).

11. Method according to any one of Claims 5-10, characterised in that said step of sending a result of said comparison to said second device (11) comprises the steps of:

- generating a message containing said result;
- ciphering said message.

12. Method according to any one of the previous claims, characterised in that said identification biometric technics comprise at least one biometric identification technic of the type selected among: face recognition, fingerprints, hand prints, voice templates, retinal images, calligraphic samples.

13. Method according to any one of Claims 2-12, characterised in that said first and second system (2), (3) are respectively a data enrolment system and a data verification system and said device (4) is a data carrier.

14. User authentication architecture bases on the use of biometric identification technics comprising:

- at least one data enrolment system (2) for generating a reference biometric template from a first biometric image of a user to be authenticated, said data enrolment system (2) comprising a Host Computer (7) to split said reference biometric template into a first and a second reference biometric template portion and for ciphering said first and second reference biometric template portion;

- at least one portable data carrier (4) associated with said user to be authenticated, said data carrier (4) comprising a memory (6a) for storing said first signed and ciphered reference biometric template portion; and

- at least one data verification system (3) comprising a memory (11a) for storing said second signed and ciphered reference biometric template portion.

15. Architecture according to Claim 14, characterised in that said data carrier (4) comprises a microprocessor (5) including a processing logic (5a) for deciphering said first and second reference biometric template portion, verification the signature and re-composing said reference biometric template from said first and second deciphered reference biometric template portion.

16. Architecture according to Claim 15, characterised in that said microprocessor (5) comprises a comparing logic (5b) to compare said re-composed reference biometric template with a template live generated by a second biometric image of the user to be authenticated, said second biometric image of the user to be authenticated being generated by the data verification system (3).

17. Portable data carrier (4) associated with a user that has to be authenticated through a user authentication architecture (1), said data carrier (4) including a microprocessor (5) comprising a memory (6) for storing a first reference biometric template portion associated with said user to be authenticated, said first reference biometric template portion being signed and ciphered, said portable data carrier being adapted to receive as input, from said user authentication architecture, a second reference

biometric template portion and a template live associated with said user to be authenticated, said second reference biometric template portion and said template live being signed and ciphered, said microprocessor (5) further comprising:

- a processing logic (5a) for deciphering said first and second reference biometric template portions and for re-composing therefrom said reference biometric template associated with said user to be authenticated;

- a comparing logic (5b) for comparing said reference biometric template re-composed with said template live and sending a result of said comparison to said user authentication architecture (1).

18. Data carrier according to Claim 17, characterised in that it comprises a substrate whose sizes are substantially rectangular.

19. Data carrier according to any one of Claims 17 or 18, characterised in that said data carrier (4) is an access card or a credit card or a debit card or an identification card or a smart card or a SIM card.

20. Data verification system (3) comprising an electronic device (11) and a portable data carrier (4) associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and ciphered;

said electronic device comprising:

- a memory (11a) adapted to store a second reference biometric template portion associated with a user to be authenticated, complementary to said first portion, said second reference biometric template portion being signed and ciphered;

- an image acquiring and processing device (12) for generating a template live;

said electronic device (11) being adapted to cipher and sign said template live, transmitting said second reference biometric template portion and said template live to said portable data carrier (4) and authenticating said user depending on the result of a comparison performed by said data carrier (4) between said template live and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first and second reference biometric template portion.

21. Program for electronic processor that can be loaded into the memory of at least one electronic processor and including program codes for performing the steps of the method according to any one of Claims 1-13 when said program is executed by said electronic processor.

ABSTRACT

The present invention refers to a user authentication method based on the use of identification biometric technics comprising the steps of:

- generating a reference biometric template from a first biometric image of a user to be authenticated;

- splitting the reference biometric template into a first and a second reference biometric template portion that can be physically separated;

- signing and ciphering the first and the second reference biometric template portion;

- storing the signed and ciphered first and the second reference biometric template portion into different memories.

(Fig.1)

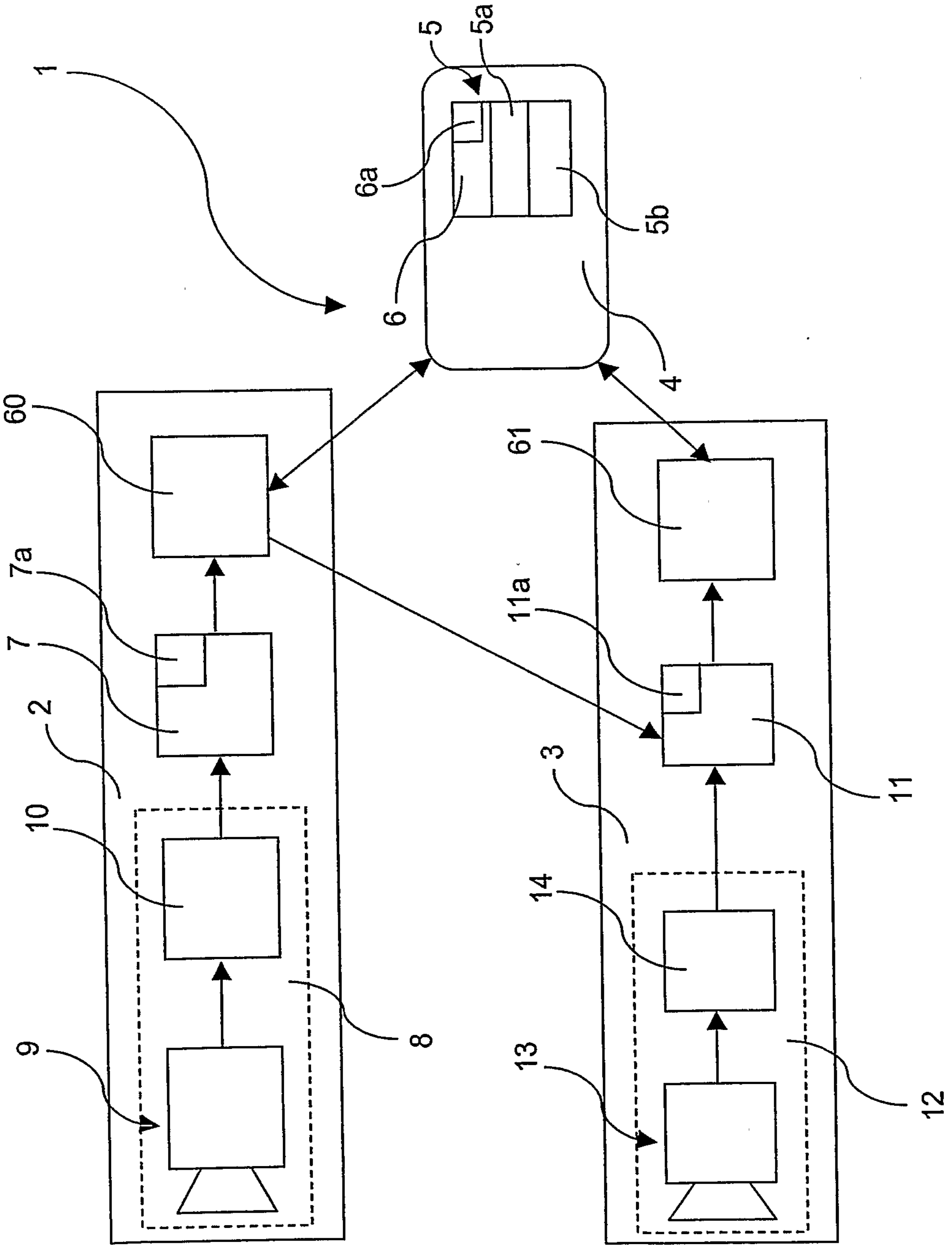

FIG. 1

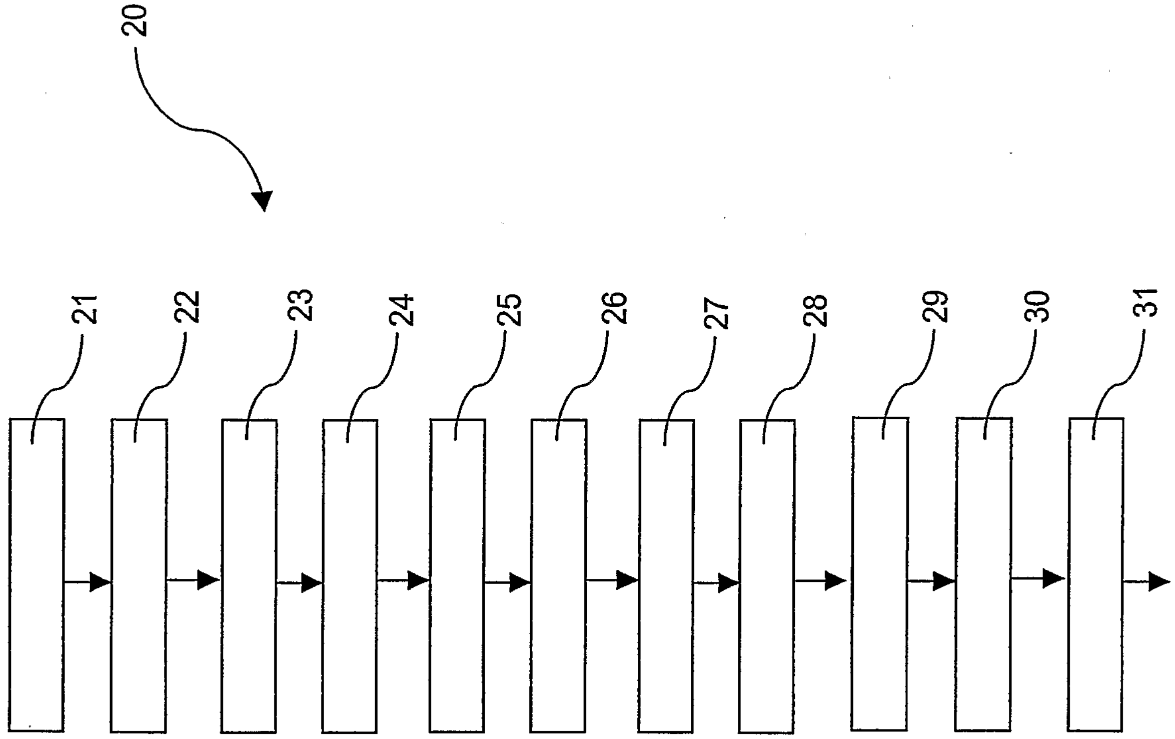

FIG. 2

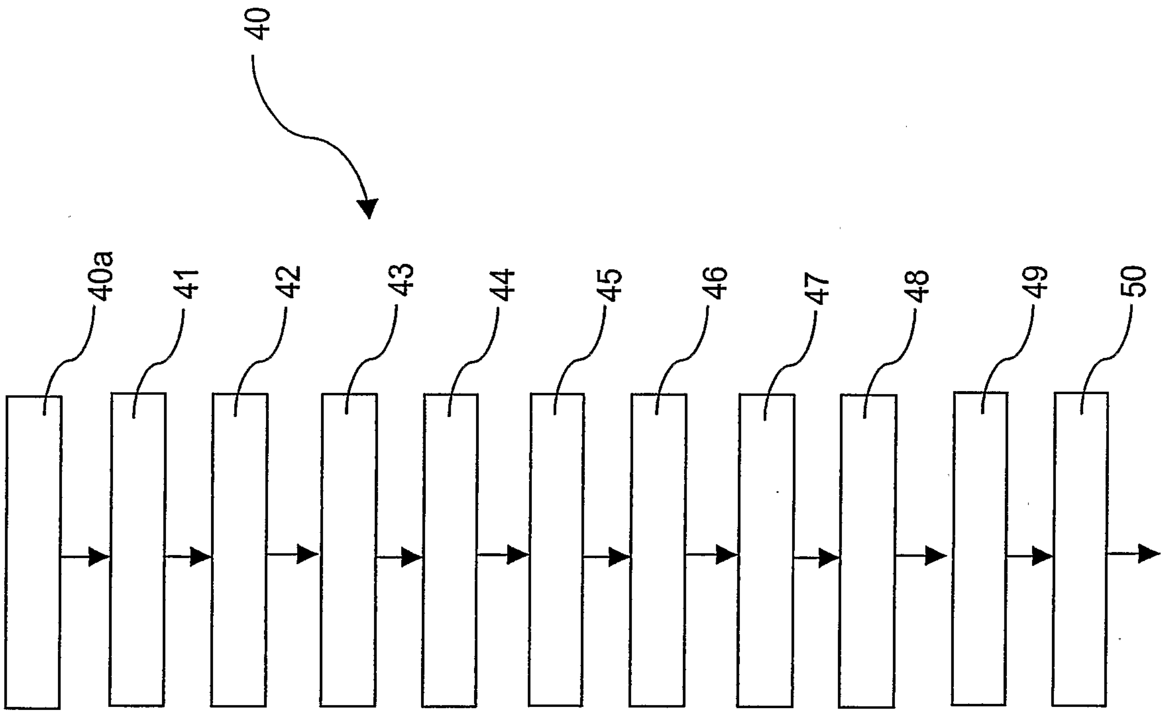

FIG.3